サイバー セキュリティ リスク評価チェックリスト テンプレート サンプル

ISO 27001 管理	実装フェーズ	タスク	遵守していますか？	備考
5	*情報セキュリティに関するポリシー*			
5.1	**情報セキュリティ管理の方向性**			
5.1.1	情報セキュリティに関するポリシー	セキュリティに関するポリシーはありますか？	☐	
		すべてのポリシーは経営陣の承認を得ていますか？	☐	
		コンプライアンスの証拠はありますか？	☐	
6	*情報セキュリティの組織*			
6.1	**情報セキュリティの役割と責任**			
6.1.1	セキュリティの役割と責任	役割と責任は決まっていますか？	☐	
6.1.2	職務分掌	職務分掌は決まっていますか？	☐	
6.1.3	関係当局との連絡	認証機関/当局よりコンプライアンス認証に関する連絡がありましたか？	☐	
6.1.4	専門組織との連絡	コンプライアンスに関して専門組織へ連絡を取りましたか？	☐	
6.1.5	プロジェクト管理における情報セキュリティ	プロジェクト管理における情報セキュリティの証拠はありますか？	☐	
6.2	**モバイル デバイスとテレワーク**			
6.2.1	モバイル デバイスに関するポリシー	モバイル デバイスに関する明確なポリシーはありますか？	☐	
6.2.2	テレワーク	リモート ワークに関する明確なポリシーはありますか？	☐	
7	*人的情報セキュリティ*			
7.1	**雇用前**			
7.1.1	選考	雇用前の従業員選考に関する明確なポリシーはありますか？	☐	
7.1.2	雇用条件	人事の雇用条件に関する明確なポリシーはありますか？	☐	
7.2	**雇用中**			
7.2.1	経営陣の責任	経営陣の責任に関する明確なポリシーはありますか？	☐	
7.2.2	情報セキュリティの意識向上、教育および訓練	情報セキュリティの意識向上、教育および訓練に関する明確なポリシーはありますか？	☐	
7.2.3	懲戒手続	情報セキュリティ関連の懲戒手続に関する明確なポリシーはありますか？	☐	

7.3	**雇用の終了および変更**			
7.3.1	雇用の終了または変更に対する責任	情報セキュリティ関連の人事の雇用の終了および変更に関する明確なポリシーはありますか？	☐	
8	***資産管理***			
8.1	**資産に対する責任**			
8.1.1	資産目録	完全な資産目録リストはありますか？	☐	
8.1.2	資産の管理責任	完全な資産の管理責任リスト	☐	
8.1.3	資産の利用規約	資産の「利用規約」に関する明確なポリシー	☐	
8.1.4	資産の返却	資産の返却に関する明確なポリシーはありますか？	☐	
8.2	**情報分類**			
8.2.1	情報分類	情報分類に関する明確なポリシーはありますか？	☐	
8.2.2	情報のラベル付け	情報のラベル付けに関する明確なポリシーはありますか？	☐	
8.2.3	資産の取り扱い	資産の取り扱いに関する明確なポリシーはありますか？	☐	
8.3	**媒体の取り扱い**			
8.3.1	取外し可能な媒体の管理	取外し可能な媒体の管理に関する明確なポリシーはありますか？	☐	
8.3.2	媒体の処分	媒体の処分に関する明確なポリシーはありますか？	☐	
8.3.3.	物理的媒体の輸送	物理的媒体の輸送に関する明確なポリシーはありますか？	☐	
9	***アクセス制御***			
9.1	**資産に対する責任**			
9.1.1	アクセス制御に関するポリシー	アクセス制御ポリシーに関する明確なポリシーはありますか？	☐	
9.1.2	ネットワークおよびネットワーク サービスへのアクセス	ネットワークおよびネットワーク サービスへのアクセスに関する明確なポリシーはありますか？	☐	
9.2	**資産に対する責任**			
9.2.1	利用者の資産登録と登録解除	利用者の資産登録と登録解除に関する明確なポリシーはありますか？	☐	
9.2.2	利用者アクセスの提供	利用者アクセスの提供に関する明確なポリシーはありますか？	☐	
9.2.3	特権アクセス権の管理	特権アクセス権の管理に関する明確なポリシーはありますか？	☐	

9.2.4	利用者の秘密認証情報の管理	利用者の秘密認証情報の管理に関する明確なポリシーはありますか？	☐	
9.2.5	利用者アクセス権のレビュー	利用者アクセス権のレビューに関する明確なポリシーはありますか？	☐	
9.2.6	アクセス権の削除または修正	アクセス権の削除または修正に関する明確なポリシーはありますか？	☐	
9.3	**利用者の責任**			
9.3.1	秘密認証情報の利用	秘密認証情報の利用に関する明確なポリシーはありますか？	☐	
9.4	**システムおよびアプリケーションのアクセス制御**			
9.4.1	情報へのアクセス制限	情報へのアクセス制限に関する明確なポリシーはありますか？	☐	
9.4.2	セキュリティに配慮したログイン手順	セキュリティに配慮したログイン手順に関する明確なポリシーはありますか？	☐	
9.4.3	パスワード管理システム	パスワード管理システムに関する明確なポリシーはありますか？	☐	
9.4.4	特権的なユーティリティ プログラムの使用	特権的なユーティリティ プログラムの使用に関する明確なポリシーはありますか？	☐	
9.4.5	プログラム ソース コードへのアクセス制御	プログラム ソース コードへのアクセス制御に関する明確なポリシーはありますか？	☐	
10	***暗号化***			
10.1	**暗号化による管理**			
10.1.1	暗号による管理策の利用に関するポリシー	暗号による管理策の利用に関する明確なポリシーはありますか？	☐	
10.1.2	鍵管理	鍵管理に関する明確なポリシーはありますか？	☐	
11	***物理的および環境的セキュリティ***			
11.1	**安全な環境**			
11.1.1	物理的セキュリティ境界	物理的セキュリティ境界に関する明確なポリシーはありますか？	☐	
11.1.2	物理的入退管理策	物理的入退管理策に関する明確なポリシーはありますか？	☐	
11.1.3	オフィス、部屋、施設のセキュリティ確保	オフィス、部屋、施設のセキュリティ確保に関する明確なポリシーはありますか？	☐	
11.1.4	外部および環境の脅威からの保護	外部および環境の脅威からの保護に関する明確なポリシーはありますか？	☐	
11.1.5	セキュリティを保つべき領域での作業	セキュリティを保つべき領域での作業に関する明確なポリシーはありますか？	☐	
11.1.6	受渡場所	受渡場所に関する明確なポリシーはありますか？	☐	

11.2.	**機器**			
11.2.1	機器の設置および保護	機器の設置および保護に関する明確なポリシーはありますか？	☐	
11.2.2	サポート ユーティリティ	サポート ユーティリティに関する明確なポリシーはありますか？	☐	
11.2.3	ケーブル配線のセキュリティ	ケーブル配線のセキュリティに関する明確なポリシーはありますか？	☐	
11.2.4	装置の保守	装置の保守に関する明確なポリシーはありますか？	☐	
11.2.5	資産の移動	資産の移動に関する明確なポリシーはありますか？	☐	
11.2.6	構外にある機器および資産のセキュリティ	構外にある機器および資産のセキュリティに関する明確なポリシーはありますか？	☐	
11.2.7	装置のセキュリティを保った処分または再利用	装置のセキュリティを保った処分または再利用に関するポリシーはありますか？	☐	
11.2.8	無人状態にある利用者装置	無人状態にある利用者装置に関する明確なポリシーはありますか？	☐	
11.2.9	クリアデスク クリアスクリーン ポリシー	クリアデスク クリアスクリーン ポリシーに関する明確なポリシーはありますか？	☐	
12	***運用セキュリティ***			
12.1	**操作手順と責任**			
12.1.1	操作手順書	操作手順書に関する明確なポリシーはありますか？	☐	
12.1.2	変更管理	変更管理に関する明確なポリシーはありますか？	☐	
12.1.3	容量・能力の管理	容量・能力の管理に関する明確なポリシーはありますか？	☐	
12.1.4	開発環境、試験環境および運用環境の分離	開発環境、試験環境および運用環境の分離に関する明確なポリシーはありますか？	☐	
12.2	**マルウェアからの保護**			
12.2.1	マルウェアに対する管理策	マルウェアに対する管理策に関する明確なポリシーはありますか？	☐	
12.3	**システムのバックアップ**			
12.3.1	バックアップ	システムのバックアップに関する明確なポリシーはありますか？	☐	
12.3.2	情報のバックアップ	情報のバックアップに関する明確なポリシーはありますか？	☐	
12.4	**ログ取得と監視**			
12.4.1	イベント ログ取得	イベント ログ取得に関する明確なポリシーはありますか？	☐	

12.4.2	ログイン情報の保護	ログイン情報の保護に関する明確なポリシーはありますか？	☐	
12.4.3	実務管理者および運用担当者の作業ログ	実務管理者および運用担当者の作業ログに関する明確なポリシーはありますか？	☐	
12.4.4	クロックの同期	クロックの同期に関する明確なポリシーはありますか？	☐	
12.5	**運用ソフトウェアの管理**			
12.5.1	運用システムに関わるソフトウェアの導入	運用システムに関わるソフトウェアの導入に関する明確なポリシーはありますか？	☐	
12.6	**技術的ぜい弱性の管理**			
12.6.1	技術的ぜい弱性の管理	技術的ぜい弱性の管理に関する明確なポリシーはありますか？	☐	
12.6.2	ソフトウェアのインストールの制限	ソフトウェアのインストールの制限に関する明確なポリシーはありますか？	☐	
12.7	**情報システムの監査に対する管理策**			
12.7.1	情報システムの監査に対する管理策	情報システムの監査に対する管理策に関する明確なポリシーはありますか？	☐	
13	***通信のセキュリティ***			
13.1	**ネットワーク セキュリティ管理**			
13.1.1	ネットワーク管理策	ネットワーク管理策に関する明確なポリシーはありますか？	☐	
13.1.2	ネットワーク サービスのセキュリティ	ネットワーク サービスのセキュリティに関する明確なポリシーはありますか？	☐	
13.1.3	ネットワークの分離	ネットワークの分離に関する明確なポリシーはありますか？	☐	
13.2	**情報転送**			
13.2.1	情報転送に関するポリシーと手順	情報転送に関するポリシーと手順に関する明確なポリシーはありますか？	☐	
13.2.2	情報転送に関する合意	情報転送に関する合意に関する明確なポリシーはありますか？	☐	
13.2.3	電子的メッセージ通信	電子的メッセージ通信に関する明確なポリシーはありますか？	☐	
13.2.4	秘密保持契約または守秘義務契約	秘密保持契約または守秘義務契約に関する明確なポリシーはありますか？	☐	
13.2.5	システムの取得、開発、保守	システムの取得、開発、保守に関する明確なポリシーはありますか？	☐	
14	***システムの取得、開発、保守***			
14.1	**情報システムのセキュリティ要求事項**			
14.1.1	情報セキュリティ要求事項の分析および仕様化	情報セキュリティ要求事項の分析および仕様化に関する明確なポリシーはありますか？	☐	

14.1.2	公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮	公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮に関する明確なポリシーはありますか？	☐	
14.1.3	アプリケーション サービスのトランザクションの保護	アプリケーション サービスのトランザクションの保護に関する明確なポリシーはありますか？	☐	
14.2	**開発プロセスとサポート プロセスのセキュリティ**			
14.2.1	社内開発	社内開発に関する明確なポリシーはありますか？	☐	
15	***サプライヤーとの関係***			
15.1.1	サプライヤーとの関係	サプライヤーとの関係に関する明確なポリシーはありますか？	☐	
16	***情報セキュリティ インシデント管理***			
16.1.1	情報セキュリティ管理	情報セキュリティ管理に関する明確なポリシーはありますか？	☐	
17	***事業継続管理の情報セキュリティの側面***			
17.1	**情報セキュリティ継続**			
17.1.1	情報セキュリティ継続	情報セキュリティ継続に関する明確なポリシーはありますか？	☐	
17.2	**冗長性**			
17.2.1	冗長性	冗長性に関する明確なポリシーはありますか？	☐	
18	***コンプライアンス***			
18.1	**法的および契約上の要件の遵守**			
18.1.1	適用法令および契約上の要求事項の特定	適用法令および契約上の要求事項の特定に関する明確なポリシーはありますか？	☐	
18.1.2	知的財産権	知的財産権に関する明確なポリシーはありますか？	☐	
18.1.3	記録の保護	記録の保護に関する明確なポリシーはありますか？	☐	
18.1.4	プライバシーおよび個人を特定できる情報の保護	プライバシーおよび個人を特定できる情報の保護に関する明確なポリシーはありますか？	☐	
18.1.5	暗号化機能に対する規制	暗号化機能に対する規制に関する明確なポリシーはありますか？	☐	
18.1	**情報セキュリティの独立したレビュー**			
18.1.1	情報セキュリティのための方針群および標準の順守	情報セキュリティのための方針群および標準の順守に関する明確なポリシーはありますか？	☐	
18.1.2	技術的順守のレビュー	技術的順守のレビューに関する明確なポリシーはありますか？	☐	

免責条項

Smartsheet がこの Web サイトに掲載している記事、テンプレート、または情報などは、あくまで参考としてご利用ください。Smartsheet は、情報の最新性および正確性の確保に努めますが、本 Web サイトまたは本 Web サイトに含まれる情報、記事、テンプレート、あるいは関連グラフィックに関する完全性、正確性、信頼性、適合性、または利用可能性について、明示または黙示のいかなる表明または保証も行いません。かかる情報に依拠して生じたいかなる結果についても Smartsheet は一切責任を負いませんので、各自の責任と判断のもとにご利用ください。

このテンプレートはサンプルとしてのみ提供されています。このテンプレートは、決して法的またはコンプライアンス上のアドバイスを意味するものではありません。このテンプレートのユーザーは、必須の情報および目的を達成するために必要な情報を見極める必要があります。